



———— CIVIL ————
INFRASTRUCTURE
———— PLATFORM ————

Activities of Super Long Term Support Kernel Workgroup in Civil Infrastructure Platform Project

Pavel Machek
CIP Kernel Maintainer, Denx

SZ Lin (林上智)
CIP Kernel Working Group Chairperson and
TSC Representative, Moxa Inc.
ELCE 2019, France, 29th Oct.

About Us



- **Pavel Machek** <pavel@denx.de>
 - Cooperating with Denx
 - Kernel hacker
 - **4096R/92DFCE96**
 - 4FA7 9EEF FCD4 C44F C585 B8C7 C060 2241 92DF CE96
- **SZ Lin (林上智)** <sz.lin@moxa.com>
 - Working for Moxa Inc.
 - Debian developer
 - Contribute to Linux and other OSS projects
 - **4096R/9561F3F9**
 - 178F 8338 B314 01E3 04FC 44BA A959 B38A 9561 F3F9

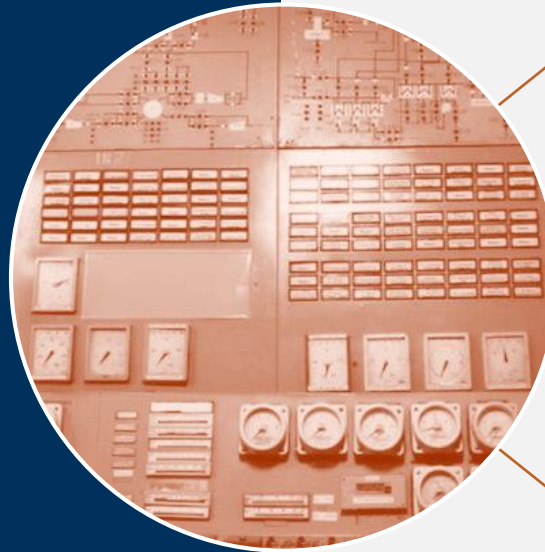
Civil Infrastructure

<https://www.airpano.com/360Degree-VirtualTour.php?3D=San-Francisco-USA>

Embedded Linux Conference Europe 2019

The key challenges

- Apply IoT concepts to industrial systems.
- Ensure quality and longevity of products.
- Keep millions of connected systems secure.



Industrial grade

- Reliability
- Functional Safety
- Real-time capabilities

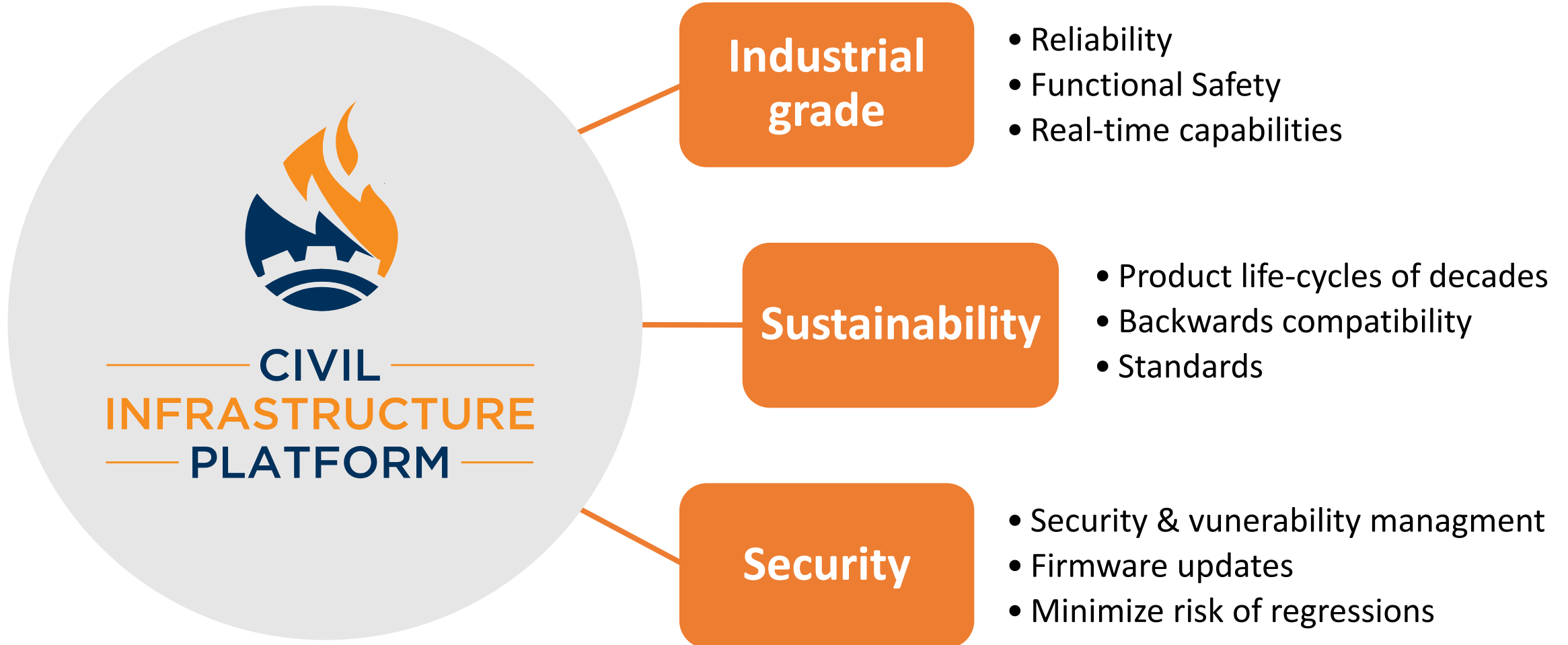
Sustainability

- Product life-cycles of decades
- Backwards compatibility
- Standards

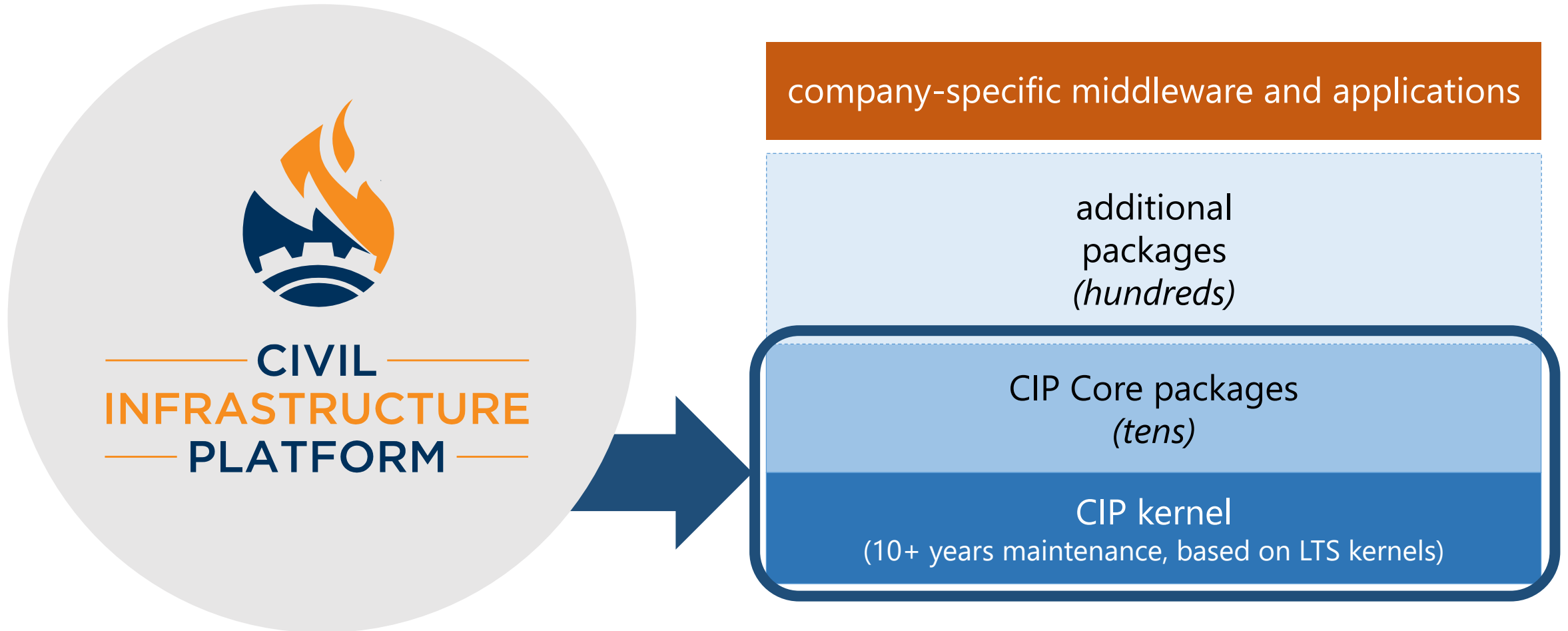
Security

- Security & vulnerability management
- Firmware updates
- Minimize risk of regressions

CIP is the Solution

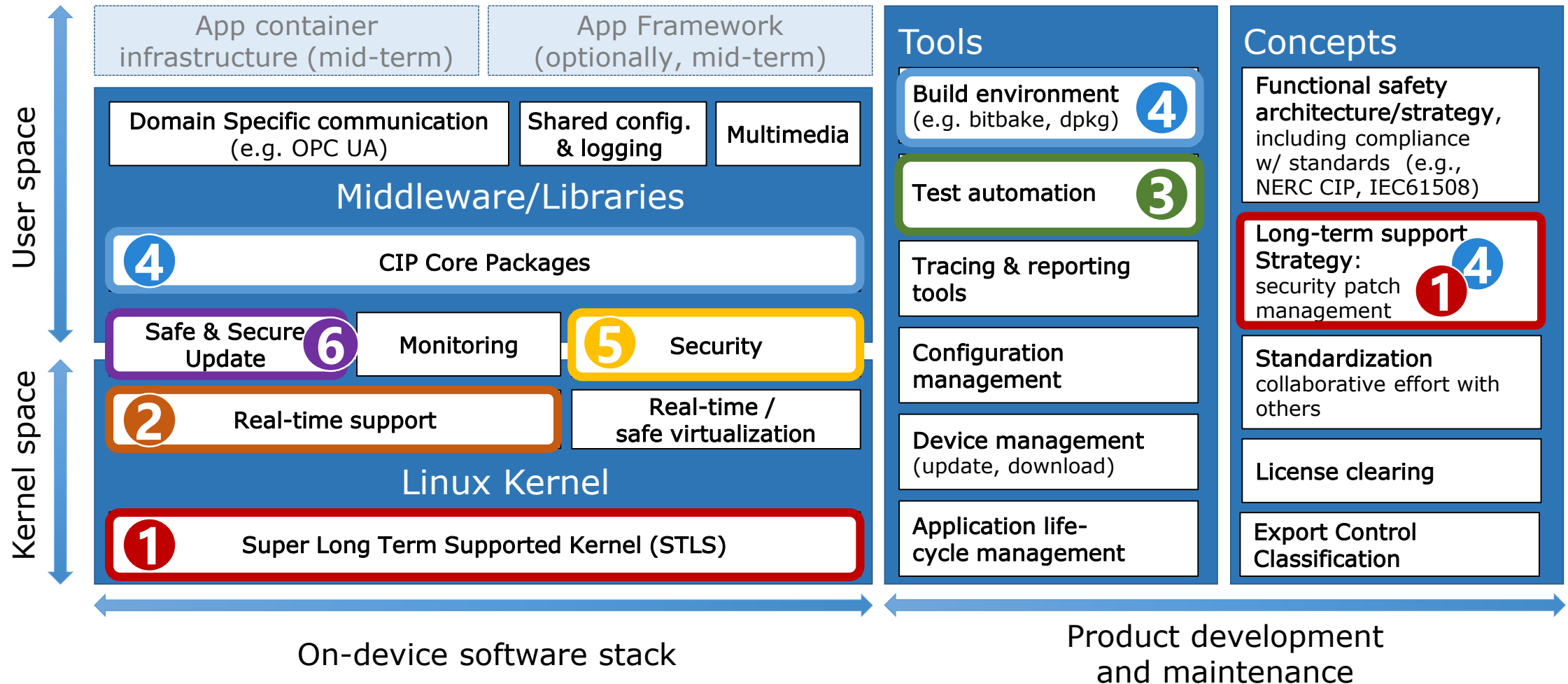


CIP is the Solution



Establishes an “Open Source Base Layer (OSBL)”

The Scope of CIP



Super Long Term Support Kernel Workgroup



- The first action taken by the CIP project is to select and maintain Linux kernels for very long time (10+ years).
- Applying the PREEMPT_RT patch to CIP Kernel, then maintaining as CIP-RT.

1	2	3	4	5	6	(*): Workgroup
SLTS kernel	Real-time	Testing	CIP Core	Security WG ^(*)	Software update WG	
✓	✓	✓	✓	✓	✓	Industrial grade
✓		✓	✓		✓	Sustainability
✓		✓	✓	✓	✓	Security

CIP Projects and its scopes

Policy and Progress

Current LTS Versions (Retrieved 22nd, Oct 2019)



Version	Maintainer	Released	Projected EOL
5.4	Greg Kroah-Hartman & Sasha Levin	2019-XX-XX	Dec, 2021
4.19	Greg Kroah-Hartman & Sasha Levin	2018-10-22	Dec, 2020
4.14	Greg Kroah-Hartman & Sasha Levin	2017-11-12	Jan, 2024
4.9	Greg Kroah-Hartman & Sasha Levin	2016-12-11	Jan, 2023
4.4	Greg Kroah-Hartman & Sasha Levin	2016-01-10	Feb, 2022
3.16	Ben Hutchings	2014-08-03	Apr, 2020

CIP SLTS Kernel Development (Upstream First Development)

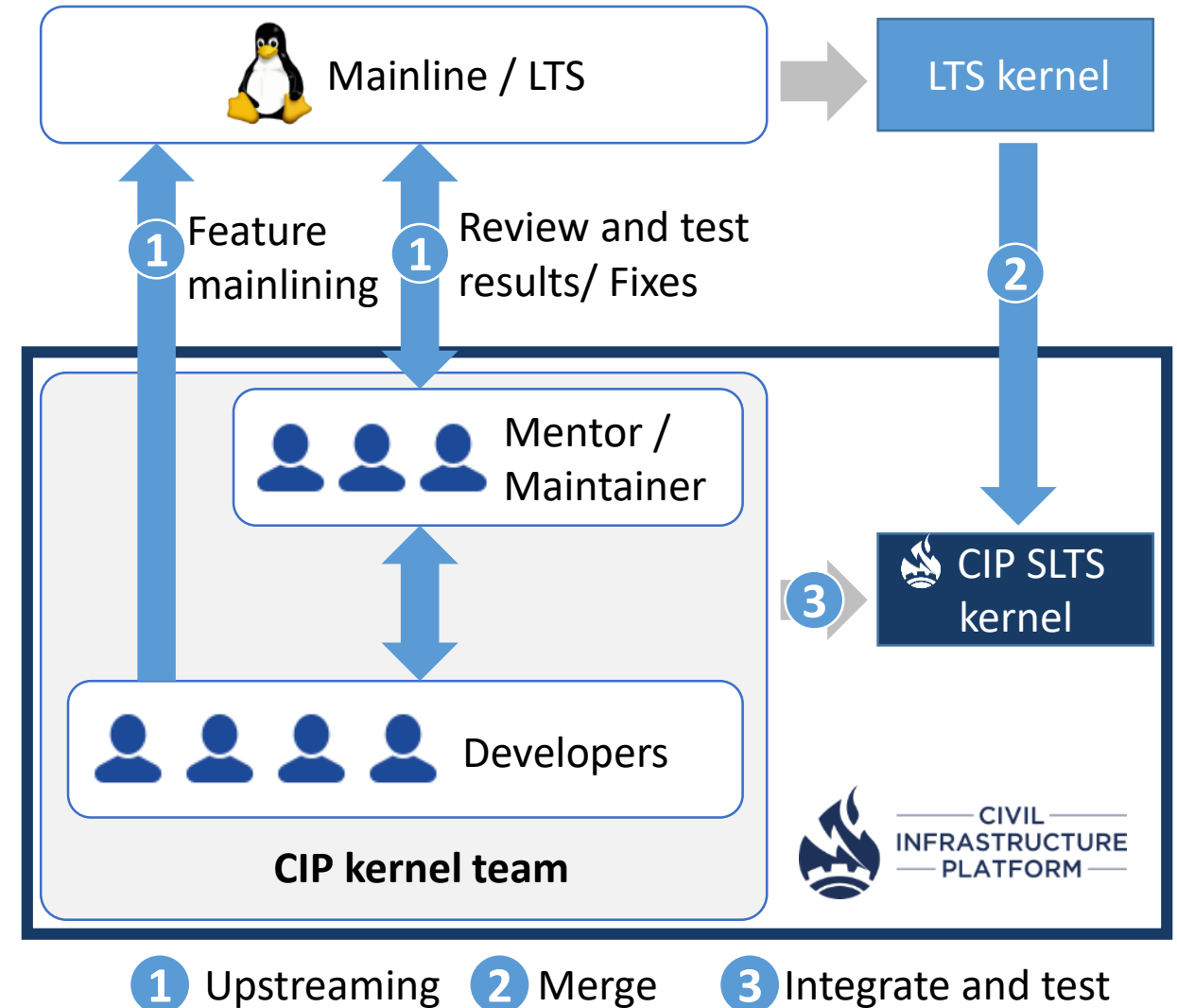


- **Goal**

- Providing CIP kernels with more than 10 years maintenance period
 - **Super Long Time Stable kernel**

- **Status**

- LTS review process participation
- CIP SLTS kernels release
 - **4.4.196-cip38**
 - **4.19.78-cip12**
- CIP kernel CVE tracker
- CIP kernel failed patches tracker



Introduction to CIP Kernel Team Member



- **Chairperson**

- SZ Lin (林上智)

- **Maintainer**

- Nobuhiro Iwamatsu
- Pavel Machek

- **Mentor**

- Ben Hutchings

Current SLTS Versions (Retrieved 22nd, Oct 2019)



Version	Maintainer	First Release	Latest Release	Projected EOL
4.19	Nobuhiro Iwamatsu & Pavel Machek	2019-01-11 • v4.19.13-cip1	2019-10-12 • v4.19.78-cip12	2029+
4.19-rt	Pavel Machek	2019-01-11 • v4.19.13-cip1-rt1	2019-10-02 • v4.19.72-cip10-rt3	2029+
4.4	Nobuhiro Iwamatsu & Pavel Machek	2017-01-17 • v4.4.42-cip1	2019-10-12 • v4.4.196-cip38	2027+
4.4-rt	Pavel Machek	2017-11-16 • v4.4.75-cip6-rt1	2019-10-02 • v4.4.190-cip36-rt25	2027+



Maintenance Policy

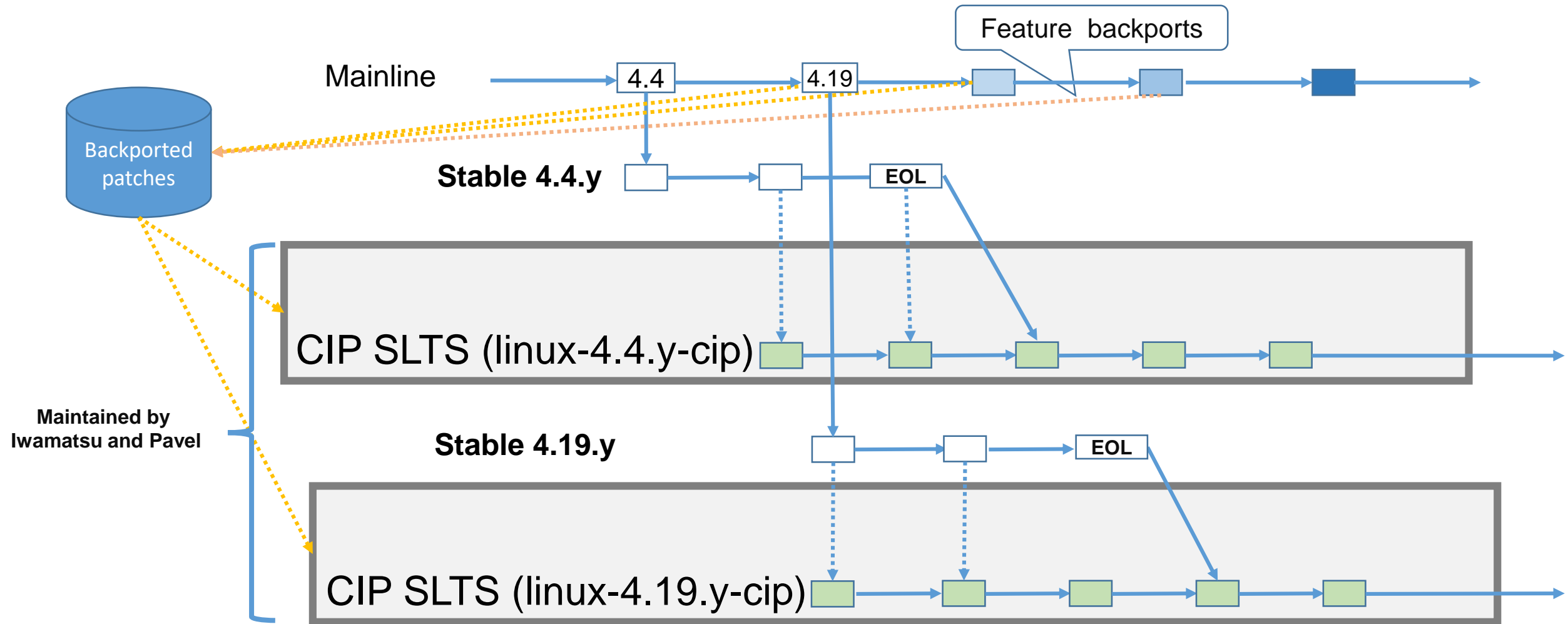
- <https://wiki.linuxfoundation.org/civilinfrastructureplatform/cipkernelmaintenance>
- Follow the stable kernel development rule as the basis
- Validation will be done by CIP test infrastructure and/or members
- Feature backports from CIP members are acceptable
 - All features has to be in upstream kernel before backport to CIP kernel
 - **CIP has “Upstream first” policy**
- The CIP Project uses the Linux Foundation Developer Certificate of Origin (DCO)



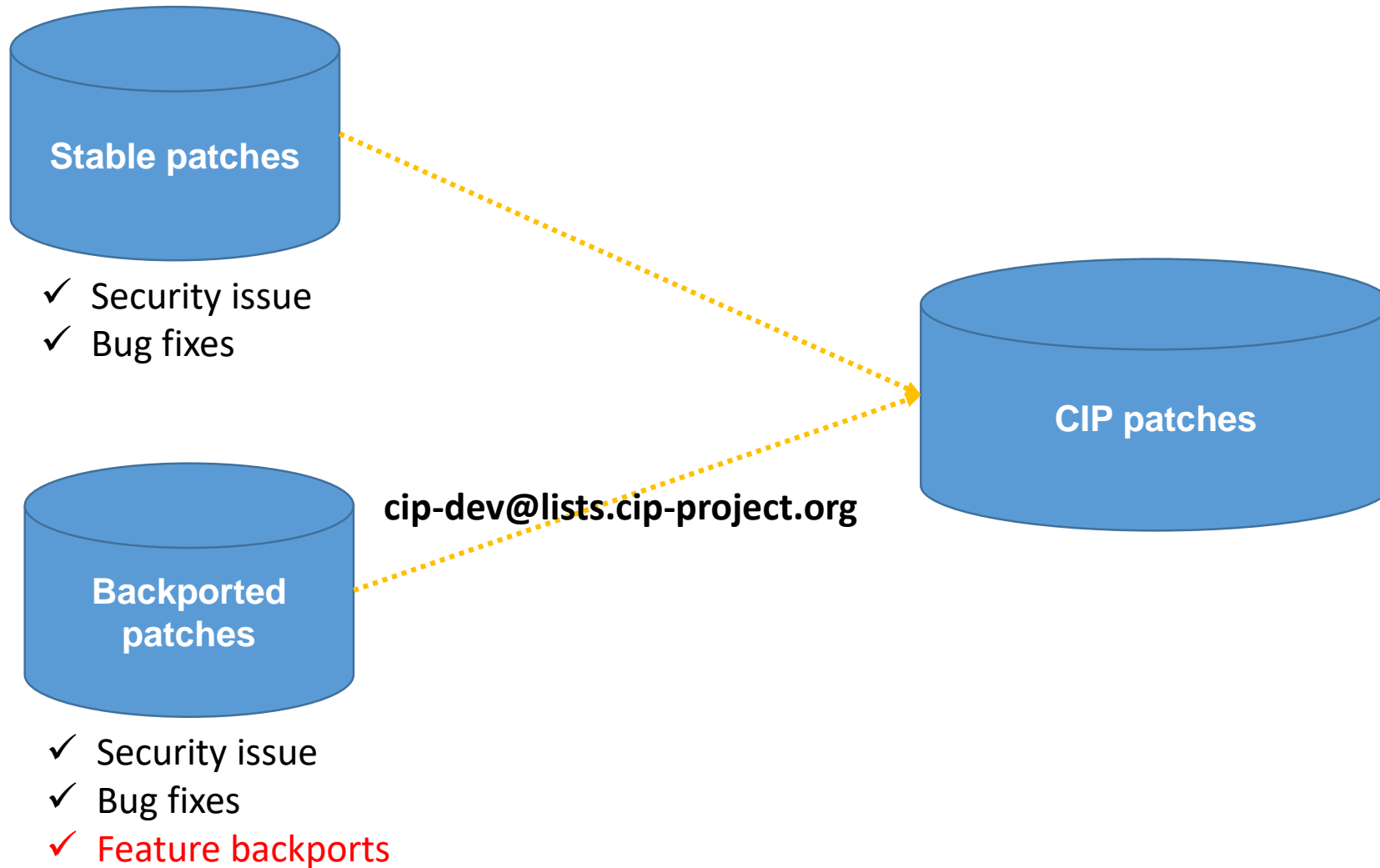
Out-of-tree drivers

- In general, all out-of-tree drivers are unsupported by CIP
- Users can use CIP kernel with out-of-tree drivers
 - If a bug is found in such a modified kernel, users will first demonstrate that it exists in the CIP kernel source release in order for the CIP maintainers to act on it.

CIP SLTS Kernel Development

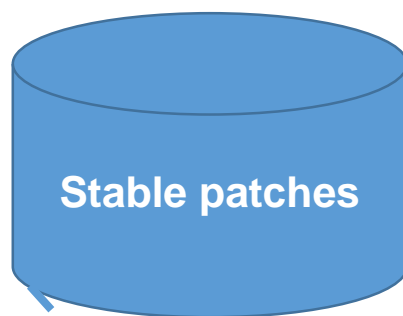


The Sources of CIP Patches



Patches Review

Stable Patches Review Participation



Stable patches

L

lts-commit-list

Star 0

Fork 0

Clone

Project ID: 11294434

Add license

120 Commits

1 Branch

0 Tags

1.1 MB Files

master

lts-commit-list /

+

History

Find file

Web IDE

 Merge branch 'master' of gitlab.com:cip-project/cip-kernel/lts-commit-list
Nobuhiro Iwamatsu authored 6 days ago

a94b154e

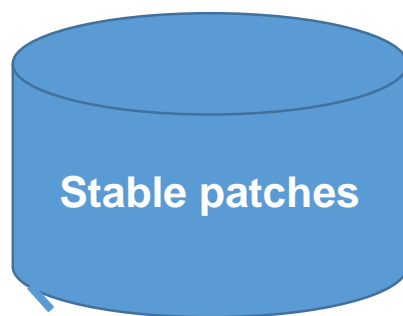


```
# Stable Kernel Patches Review Status
Please list your name and review result below the patch item

* UR: Under Review
* ACK: Acknowledge (if the patch is accepted)
* TBB: To be backported (if other patches should be also backported)
* NAK: Negative acknowledge (if the patch is rejected, please list the reason)
* IGN: Patch was not reviewed as it is out of scope for CIP project
```

Review Stable Patches

Stable Patches Review Participation



Kernel 4.4

```
## v4.4.196
- c61ebb668f2c Linux 4.4.196

ACK: iwamatsu

- 2e486758901d NFC: fix attrs checks in netlink interface

ACK: iwamatsu

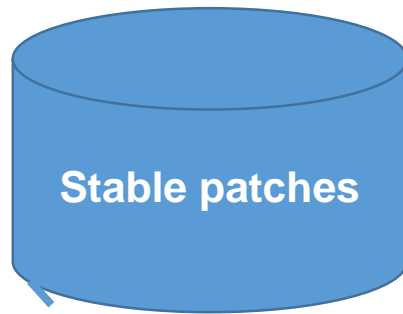
- ac375073bb39 smack: use GFP_NOFS while holding inode_smack::smk_lock
```

Kernel 4.19

```
## v4.19.77
- 6cad9d0 Linux 4.19.77
- 2c60da9 drm/amd/display: Restore backlight brightness after system resume
ACK: pavel
- 4d8bdf7 mm/compaction.c: clear total_{migrate,free}_scanned before scanning a new zone
ACK: pavel
- 5bead06 fuse: fix deadlock with aio poll and fuse_iqueue::waitq.lock
UR: pavel -- bad according to Eric Biggers
- bbe3e20 md/raid0: avoid RAID0 data corruption due to layout confusion.
UR: pavel -- should this be per-array not per-module?
- 4290a9e CIFS: Fix oplock handling for SMB 2.1+ protocols
ACK: pavel
- a3a1508 CIFS: fix max ea value size
```

Review Stable Patches

Stable Patches Review Participation



Reviewed by Pavel for 4.19-stable

```
> --- a/drivers/infiniband/core/restrack.c
> +++ b/drivers/infiniband/core/restrack.c
> @@ -209,7 +209,7 @@ void rdma_restrack_del(struct rdma_restr
>      struct ib_device *dev;
>
>      if (!res->valid)
> -         return;
> +         goto out;
>
>      dev = res_to_dev(res);
>      if (!dev)
> #         return;
```

This test does return, does it need to go through 'goto out', too? (I see it should not happen, but...)

```
> @@ -222,8 +222,10 @@ void rdma_restrack_del(struct rdma_restr
>      down_write(&dev->res.rwsem);
>      hash_del(&res->node);
>      res->valid = false;
> +      up_write(&dev->res.rwsem);
> +
> +out:
>      if (res->task)
>          put_task_struct(res->task);
> -      up_write(&dev->res.rwsem);
> }
```

Mainline says res->task = NULL is needed there, see fe9bc1644918aa1d.

Best regards,

Pavel

Review Stable Patches

Difference Between -stable Kernel Rules and Rules Imposed in Practice



a) It or an equivalent fix must already exist in Linus' tree (upstream).

Enforced. Strong preference is given to merging exactly the same patch as in upstream.

b) It must be obviously correct and tested.

Preference is given to a): buggy patch is merged, then fix is merged as followup.

c) It must fix a real bug that bothers people (not a, "This could be a problem..." type thing).

Anything that looks like a bugfix is merged, includes trivial memory leaks that leak few bytes per boot and missing of_node_put().

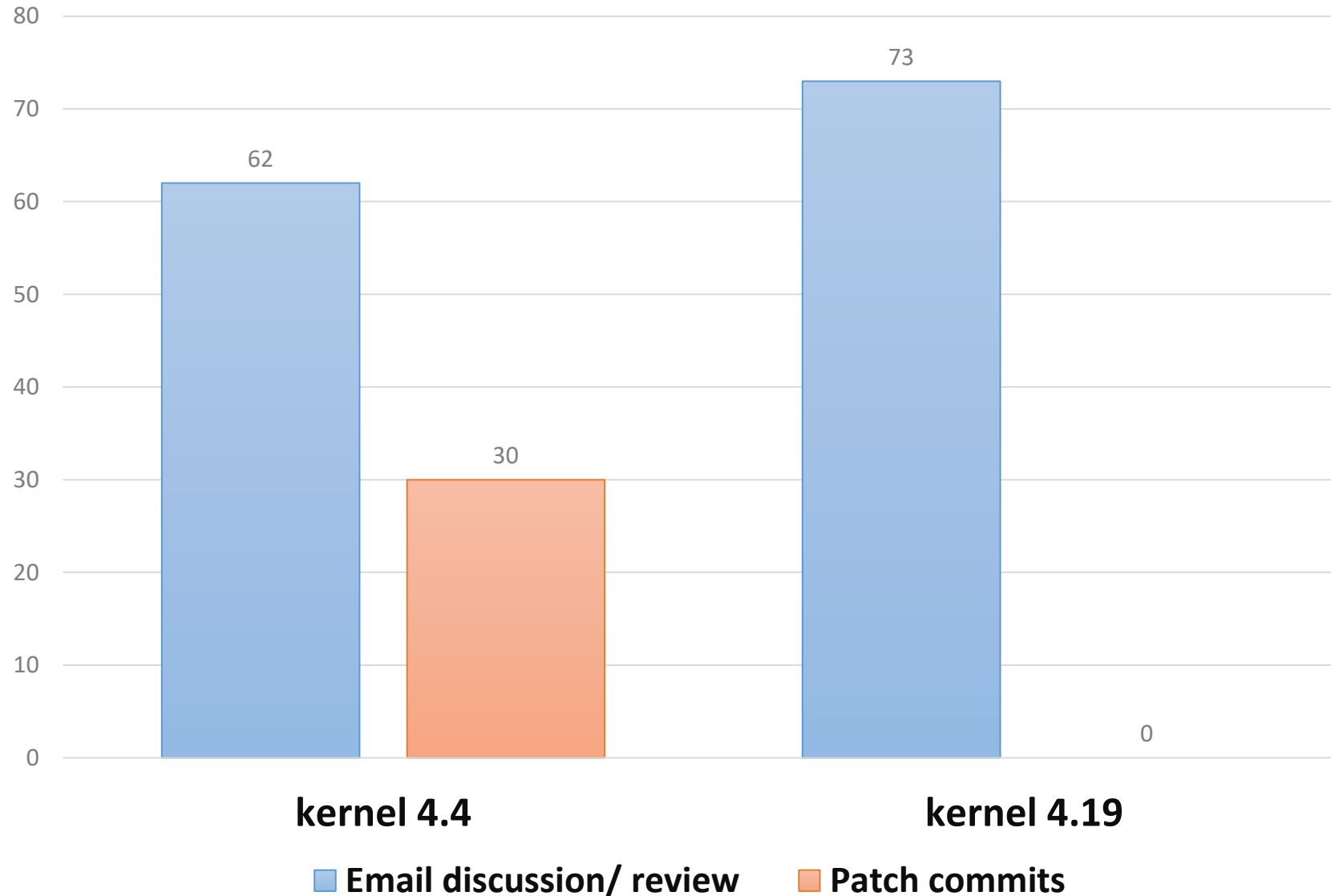
d) It must fix a problem that causes a build error (...), an oops, a hang, data corruption, a real security issue, or some "oh, that's not good" issue. In short, something critical.

Build-time warnings, run-time warnings, confusing printk messages and loglevel changes for printk messages are applied.

e) It cannot contain any "trivial" fixes in it (spelling changes, whitespace cleanups, etc).

Certainly not enforced. There is preference to taking patches from mainline with no changes.

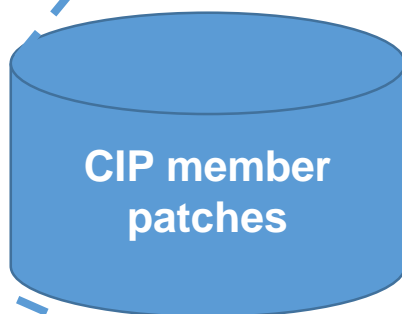
CIP Kernel Team Contribution to Upstream Statistics (Retrieved 25th , Oct 2019)



CIP Members Patches Review Participation



Review CIP Member Patches



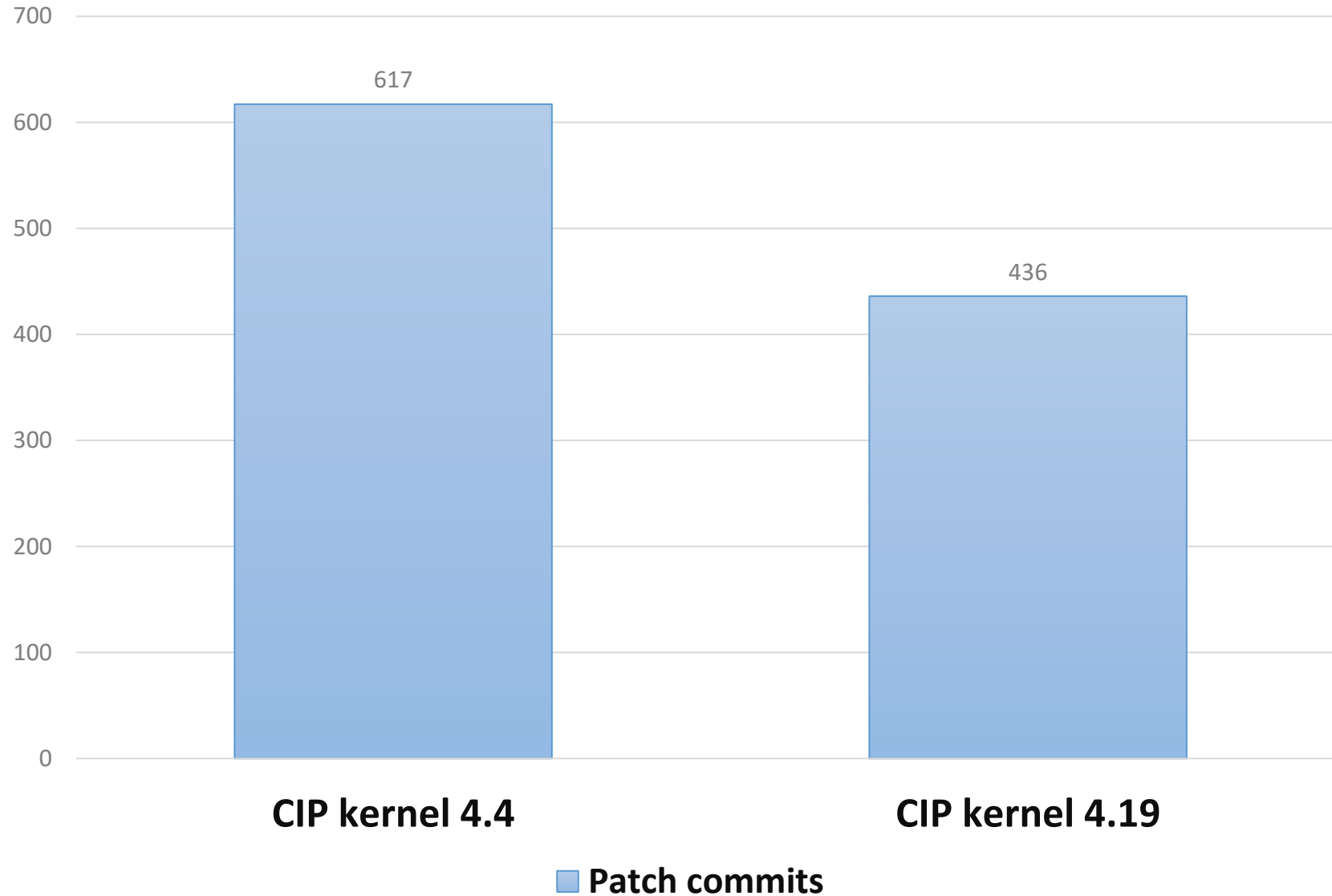
Kernel 4.4

```
[cip-dev] [PATCH 4.4-cip] ARM: dts: socfpga: Rename  
socfpga_cyclone5_de0_{socket, nano_soc} Jan Kiszka  
[cip-dev] [PATCH 4.4-cip] ARM: dts: socfpga: Rename  
socfpga_cyclone5_de0_{socket, nano_soc} Nobuhiro Iwamatsu
```

Kernel 4.19

```
[cip-dev] [PATCH 4.19.y-cip 0/4] Add USB support Biju Das  
[cip-dev] [PATCH 4.19.y-cip 0/4] Add USB support Pavel Machek  
[cip-dev] [PATCH 4.19.y-cip 0/4] Add USB support Pavel Machek
```


Feature Backported Patches Statistics in CIP Kernel

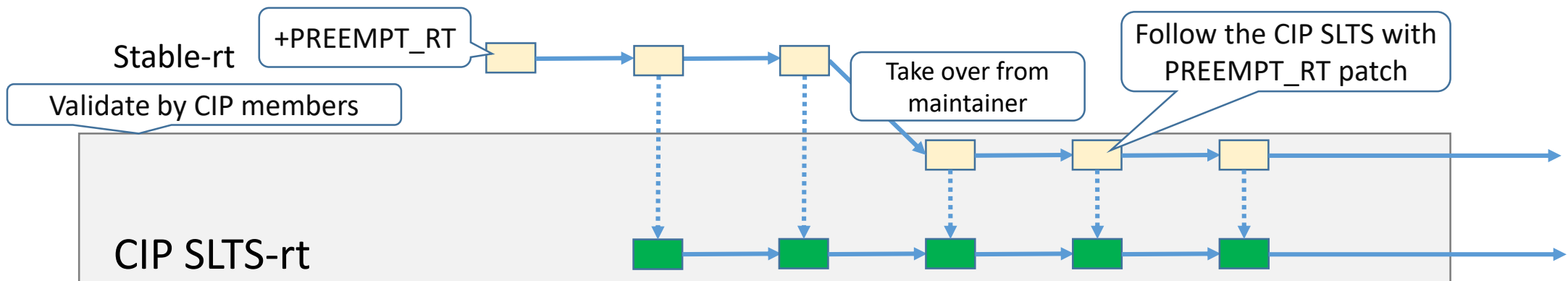


CIP SLTS Real-time Support



CIP SLTS+PREEMPT_RT (will be separately maintained by CIP members)

- CIP kernel tree based on linux-stable-rt and patches from CIP SLTS
- Validation will be done by CIP



CIP SLTS Real-time Support



- CIP has become a Gold Member of the Real Time Linux Project



- What's next
 - Work together with the RTL Project
- More information
 - <https://wiki.linuxfoundation.org/realtime/rtl/start>

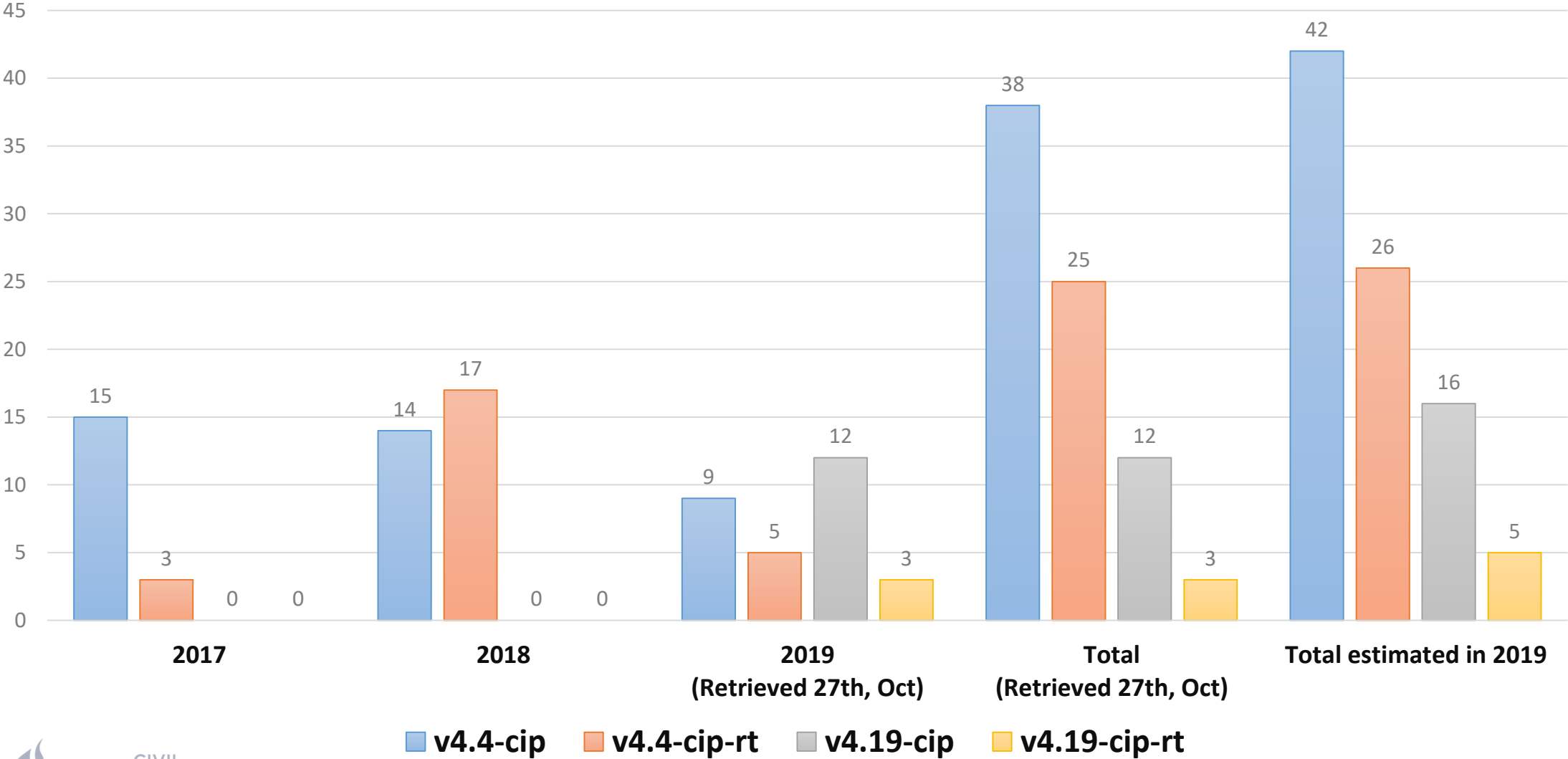
CIP SLTS Kernel Release Policy



<u>Release regularly</u>	<u>Release on demand</u>
Release 4.19 twice a month and 4.4 once a month (Effective June, 2019) <ul style="list-style-type: none">• Kernel 4.19<ul style="list-style-type: none">• second and fourth Fridays of the month• Kernel 4.4<ul style="list-style-type: none">• second Friday of the month	It depends on critical bug/ security fix
Release 4.19-rt twice a month and 4.4-rt once every two months (Effective Nov, 2019)	Ditto

Note: Difficult to estimate actual release date because of number of patches depends on each stable release

CIP Kernel and Real-time Kernel Release Statistics





Introduction to "cip-kernel-sec"



- This project tracks the status of security issues, identified by CVE ID, in mainline, stable, and other configured branches.


[cip-project](#) > [cip-kernel](#) > [cip-kernel-sec](#) > [Details](#)



cip-kernel-sec 
Project ID: 3189019
[Linux](#) [Kernel](#) [Cve](#) + 1 more

[📄 LICENSE](#) [🔗 284 Commits](#) [🌿 1 Branch](#) [🏷️ 0 Tags](#) [📁 1.5 MB Files](#)

Linux kernel CVE tracker




Auto DevOps
It will automatically build, test, and deploy your application based on a predefined CI/CD configuration.
[Learn more in the Auto DevOps documentation](#)
[Enable in settings](#)

master

cip-kernel-sec /

+

[History](#) [🔍 Find file](#) [Web IDE](#) [📄](#)



Merge branch 'bwh/update-issues' into 'master' [...](#)
SZ Lin (林上智) authored 1 week ago

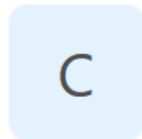
f2989df1 [📄](#)







The Maintenance Scope of "cip-kernel-sec" – “cip-kernel-config”






- The security issues are determined to be fixed base on kernel configurations provided by CIP members

 cip-project >  cip-kernel > cip-kernel-config > Details



cip-kernel-config 
Project ID: 6052798
 Linux  Kernel  Cip

☆ Star 1 Clone ▾


 **GNU GPLv2**  89 Commits  4 Branches  0 Tags  502 KB Files


Kernel configurations provided by CIP Members



master ▾


cip-kernel-config

History

 Find file

 ▾

 Merge branch 'iwamatsu/update-configs-renesas' into 'master' 

c4f7a24b 

Nobuhiro Iwamatsu authored 1 week ago

CVE Issue Format - Supported by CIP



```
description: 'netfilter: nfnetlink_cthelper: Add missing permission checks'
references:
- https://patchwork.kernel.org/patch/10089373/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17448
- https://git.kernel.org/pub/scm/linux/kernel/git/pablo/nf.git/commit/?id=4b380c42f7d00a395feede754f0bc2292eebe6e5
- https://usn.ubuntu.com/usn/usn-3617-1
- https://usn.ubuntu.com/usn/usn-3617-2
- https://usn.ubuntu.com/usn/usn-3617-3
- https://usn.ubuntu.com/usn/usn-3619-1
- https://usn.ubuntu.com/usn/usn-3620-1
- https://usn.ubuntu.com/usn/usn-3620-2
- https://usn.ubuntu.com/usn/usn-3619-2
- https://usn.ubuntu.com/usn/usn-3632-1
comments:
  Debian-bwh: |-
    This is mitigated in Debian by unprivileged user namespaces being
    default-disabled.
introduced-by:
  mainline: [12f7a505331e6b2754684b509f2ac8f0011ce644]
fixed-by:
  linux-3.16.y: [fad6474d43e985338e4c2b3bb1a7668cca1f041a]
  linux-3.18.y: [f4ba1d0e4366d63d1d09c024e8befc99c642e84b]
  linux-4.1.y: [6d752a482cf7ce18ca96abaf0a159e801d4c38e8]
  linux-4.14.y: [671624872144abc37bc5e8f3b27987890f6e87f3]
  linux-4.4.y: [a359a437fbc6bb08aa9cc8e25ef4ac3b77ca727b]
  linux-4.4.y-cip: [a359a437fbc6bb08aa9cc8e25ef4ac3b77ca727b]
  linux-4.4.y-cip-rt: [a359a437fbc6bb08aa9cc8e25ef4ac3b77ca727b]
  linux-4.9.y: [2c3184ea80322347287bc7e57f782d77f478e73c]
  mainline: [4b380c42f7d00a395feede754f0bc2292eebe6e5]
```

Issue Format - YAML

CVE Issue Format – Unsupported by CIP




```
description: 'IB/mlx5: Fix leaking stack memory to userspace'
references:
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20855
- https://cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.18.7
- https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=0625b4ba1a5d4703c7fb01c497bd6c156908af00
- https://github.com/torvalds/linux/commit/0625b4ba1a5d4703c7fb01c497bd6c156908af00
comments:
  Debian-bwh: |-
    Introduced in Linux 4.17 by commit 41d902cb7c32 "RDMA/mlx5: Fix
    definition of mlx5_ib_create_qp_resp".
introduced-by:
  mainline: [41d902cb7c326d711674977763c4b30df87611bc]
fixed-by:
  mainline: [0625b4ba1a5d4703c7fb01c497bd6c156908af00]
ignore:
  linux-4.19.y-cip: No member enables the mlx5_ib driver
  linux-4.19.y-cip-rt: No member enables the mlx5_ib driver
  linux-4.4.y-cip: No member enables the mlx5_ib driver
  linux-4.4.y-cip-rt: No member enables the mlx5_ib driver
```


Introduction to "classify-failed-patches"













- This project tracks the status of failed patches, and classifies patches into “applied” and “ToApply” types.


cip-project > cip-kernel > classify-failed-patches > Details




classify-failed-patches 
Project ID: 12455807


  Star 0  Fork 1  Clone 

 MIT License  8 Commits  1 Branch  0 Tags  2 MB Files




Auto DevOps
It will automatically build, test, and deploy your application based on a predefined CI/CD configuration.
[Learn more in the Auto DevOps documentation](#)
[Enable in settings](#)


master 



classify-failed-patches / 


History

 Find file

Web IDE



 Update data 
Nobuhiro Iwamatsu authored 2 months ago

c855d48f 



Introduction to "classify-failed-patches"



Applied patches

```
[APPLIED] arm64: Disable unhandled signal log messages by default
56b57bd20f5bcdd353eacf7b7c41ee18ffe0c963 arm64: Disable unhandled signal log messages by default
[APPLIED] ARC: hide unused function unw_hdr_alloc
4d28512bfca84456b6f65e6800c003cf0810480b ARC: hide unused function unw_hdr_alloc
[APPLIED] btrfs: Ensure replaced device doesn't have pending chunk allocation
986543fcf50c8a3681be44cac42dc498fe25ab34 btrfs: Ensure replaced device doesn't have pending chunk allocation
[APPLIED] btrfs: Ensure replaced device doesn't have pending chunk allocation
986543fcf50c8a3681be44cac42dc498fe25ab34 btrfs: Ensure replaced device doesn't have pending chunk allocation
[APPLIED] btrfs: Ensure replaced device doesn't have pending chunk allocation
986543fcf50c8a3681be44cac42dc498fe25ab34 btrfs: Ensure replaced device doesn't have pending chunk allocation
[APPLIED] btrfs: Ensure replaced device doesn't have pending chunk allocation
986543fcf50c8a3681be44cac42dc498fe25ab34 btrfs: Ensure replaced device doesn't have pending chunk allocation
```

To be Applied Patches

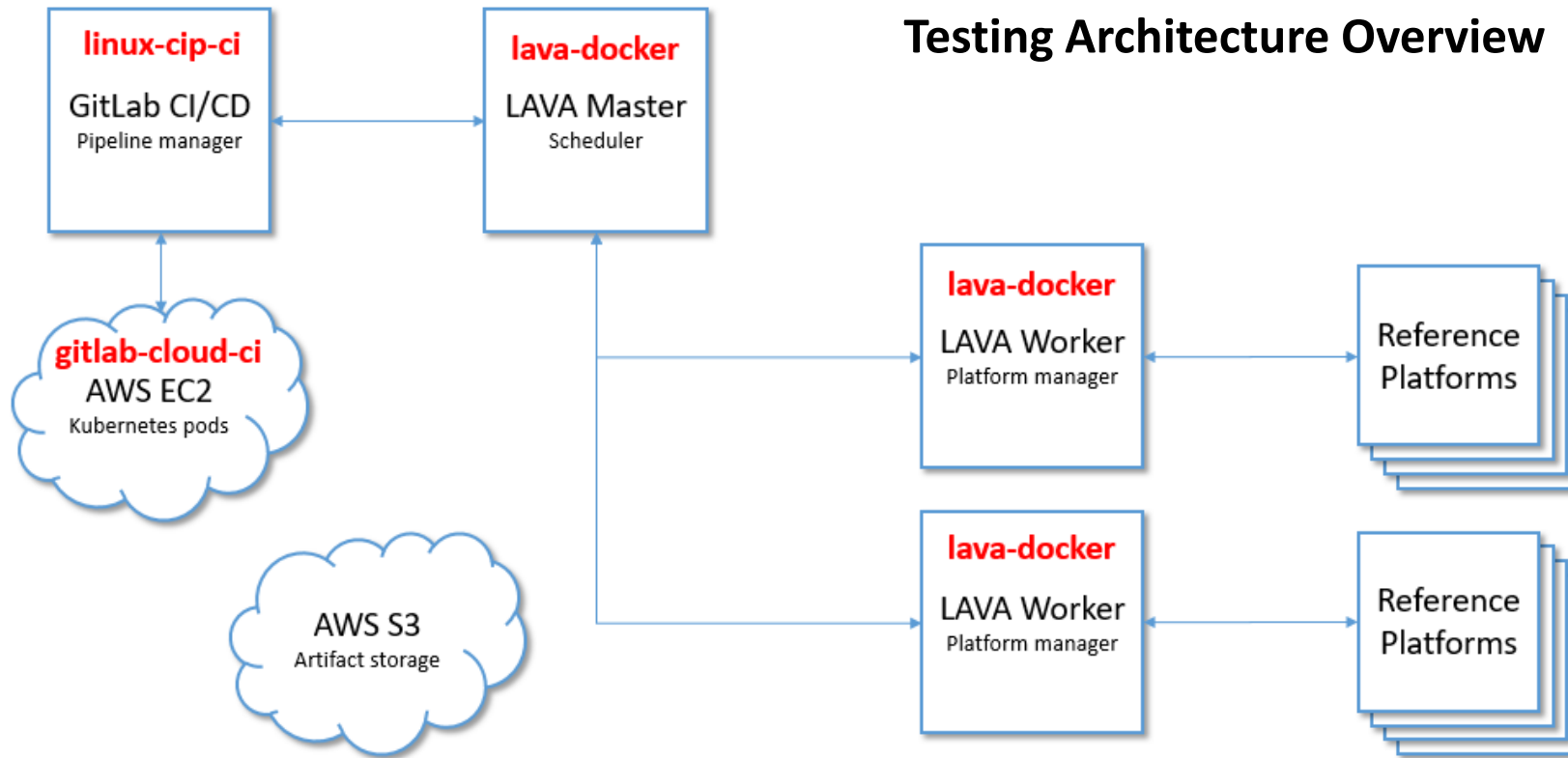
```
[TOAPPLY] inet: update the IP ID generation algorithm to patch 355b98553789b646ed97ad801a619ff898471b92 standards.
[TOAPPLY] scsi: ufs: Fix RX_TERMINATION_FORCE_ENABLE define value
[TOAPPLY] inet: update the IP ID generation algorithm to patch 355b98553789b646ed97ad801a619ff898471b92 standards.
[TOAPPLY] IB/hfi1: Failed to drain send queue when QP is put into error state
[TOAPPLY] arm64: mm: Ensure tail of unaligned initrd is reserved
[TOAPPLY] fs/proc/task_mmu.c: fix uninitialized variable warning
[TOAPPLY] tpm: Fix the type of the return value in calc_tpm2_event_size()
[TOAPPLY] block: bio_map_user_iov should not be limited to BIO_MAX_PAGES
[TOAPPLY] clk: ingenic/jz4725b: Fix parent of pixel clock
[TOAPPLY] i2c-piix4: Add Hygon Dhyana SMBus support
[TOAPPLY] TTY: serial_core, add ->install
```

Testing

CIP Testing Talk at CIP Mini Summit



- **Thursday in CIP Mini Summit**
 - 8:00 – 13:00 @ Lyon Convention Centre



Summary



- **Routine tasks**

- The frequency of CIP kernel release
 - The kernel of
 - **4.4 will be released at least once** and **4.19 will be released at least twice every month**
 - **4.4-rt will be released at least once every two months** and **4.19-rt will be released at least twice a month**
 - Failed patch tracker
 - Linux kernel CVE tracker

- **Occasional tasks**

- Build up kernel and rt-kernel testing
- Define and update the wiki for kernel maintenance scope

Weekly Regular Online Meeting



- CIP IRC weekly meeting – **Every Thursday UTC (GMT) 09:00**

US-West	US-East	UK	DE	TW	JP
02:00	05:00	09:00	10:00	17:00	18:00

- **Channel:**

* `irc:chat.freenode.net:6667/cip`

- The meeting will take 30 min although it can be extended to an hour if it makes sense and those involved in the topics can stay. Otherwise, the topic will be taken offline or in the next meeting.

CIP Kernel Workgroup Repository



- **CIP Linux kernel & real-time kernel**
 - <https://git.kernel.org/pub/scm/linux/kernel/git/cip/linux-cip.git>
- **CIP Linux kernel CVE tracker**
 - <https://gitlab.com/cip-project/cip-kernel/cip-kernel-sec>
- **CIP Linux kernel failed patches tracker**
 - <https://gitlab.com/cip-project/cip-kernel/classify-failed-patches>

Contact Information and Resources



To get the latest information, please contact:

- CIP Mailing List: cip-dev@lists.cip-project.org

Other resources

- Twitter: [@cip_project](https://twitter.com/cip_project)
- CIP Web Site: <https://www.cip-project.org>
- CIP News: <https://www.cip-project.org/news/in-the-news>
- CIP Wiki: <https://wiki.linuxfoundation.org/civilinfrastructureplatform/>
- CIP Source Code
 - CIP repositories hosted at kernel.org: <https://git.kernel.org/pub/scm/linux/kernel/git/cip/>
 - CIP GitLab: <https://gitlab.com/cip-project>

CIP Talks at ELCE, CIP Mini Summit, and ATS



- **Today (ELCE)**

- 15:15 @ Tête d'Or 2 (CIP)

Open Source Projects to Live long and Prosper: Linux for Smart Infrastructure and Industry - Yoshitake Kobayashi, Toshiba Corporation & Urs Gleim, Siemens AG

- **Thursday in CIP Mini Summit**

- 8:00 – 13:00 @ Lyon Convention Centre

- https://www.cvent.com/Events/Register/RegNumConfirmation.aspx?e=66d78d44-9d3c-4c92-85fa-a87ef8e8b62b&_ga=2.224040339.985516515.1571730868-505872952.1553045385

- **Thursday in Automated Testing Summit (ATS)**

- 15:10 @ Rhone 3AB (CIP Testing)

A Guide to CIP Testing - Chris Paterson, Renesas Electronics Europe & Michael Adler, Siemens AG

Please Visit CIP Booth!

Place: FORUM 4/5 Sponsor Showcase



“CIP mini-summit” will be held on Oct. 31th (Thu),
but sold out already, thank you!



Join us

CIP for sustainable Smart Cities with Open Source Software



———— CIVIL ————
INFRASTRUCTURE
———— PLATFORM ————

RENESAS

SIEMENS

TOSHIBA

CodeThink


cybertrust

HITACHI
Inspire the Next

MOXA®

Plat'Home
There, we are. Internet of Things

Question?



Thank you



References



- *How to make Smart Cities stay smart with Open Source Projects*, OSS-J 2019, **Yoshitake Kobayashi**
- *The Activity of the Security Working Group in the CIP Project*, OSS-J 2019, **Takehisa Katayama**
- *Debian and Yocto Project based Long-term Maintenance Approaches for Embedded Products*, ELCE 2019, **Jan Kiszka and Kazuhiro Hayashi**